NDIA Cybersecurity for Advanced Manufacturing Public Forum

August 18, 2016

Technology Solutions Team

Ms. Heather Moyer

Technology Solutions Team

Robert Badgett Consultant	**Anitha Raj** ARAR Technology	**Devu Shila** United Technologies Research Center
Vicki Barbur Consultant	**Craig Rieger** Idaho National Laboratory	**Tim Shinbara** The Association for Manufacturing Technology
Team Lead: Heather Moyer Consultant	**Frank Serna** DRAPER	**Janet Twomey** Wichita State University

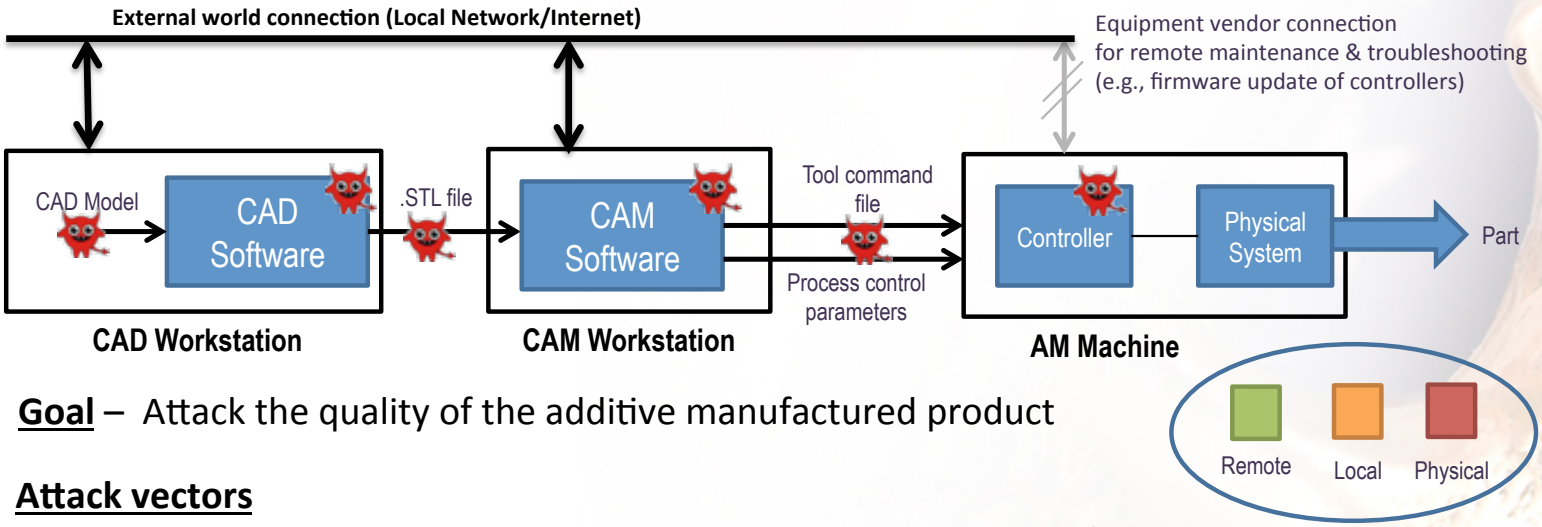
Objective

Our team will establish an initial baseline of available and emerging technology solutions to improve cybersecurity in the DIB and deliver a Recommendations Report suggesting additional technology-based concepts that should be explored.

- **Short-Term:** What can we adapt from IT to better secure OT (especially legacy manufacturing systems)?
- **Mid-Term:** What research is being (or should be) conducted that will provide additional solutions to close security gaps and how do we accelerate commercialization?
- **Long-Term:** How do we design smart manufacturing systems to mitigate cybersecurity impacts?

Current Status

Use Cases: Developed representative manufacturing scenarios for Confidentiality, Integrity, and Availability use cases. Analyzing remote, local, and physical attack vectors and conventional mitigation strategies.



Goal – Attack the quality of the additive manufactured product

Attack vectors

- Rogue designers inserting malicious logic into the CAD model, STL file, or Tool command file
- 3rd party models or files embedded with unwanted logic
- Malicious 3rd party CAD/CAM software that inserts extraneous or deletes logic into the files
- Tampers models/files/control parameters via Malware infection (by exploiting insecure external communications and software vulnerabilities of CAD/CAM software or OS)
- Modifying files or process control parameters by exploiting insecure local area communications
- Update controller firmware by exploiting insecure physical interfaces such as USB

Current Status (cont.)

SME Interviews: Engaging subject matter experts and end users (both large and small) to solicit first hand input on awareness, issues, technology and economic challenges, and best practices.

Literature Review: Identified approximately a dozen directly relevant research papers focused on cybersecurity in the manufacturing environment, but few with proven solutions.

We Need Your Input!

- If you are conducting relevant solution research in this area
- If you have a unique technology solution that could have broad impact across the DIB
- If you have identified a critical manufacturing cybersecurity issue that would benefit from government/industry collaboration